POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

FUNDACJI BEZ LUKRU I CUKRU

Rozdział I

Postanowienia ogólne

§ 1

1. Niniejsza Polityka bezpieczeństwa danych osobowych, zwana dalej „Polityką", określa zasady przetwarzania i ochrony danych osobowych w Fundacji Bez Lukru i Cukru.
2. Celem Polityki jest zapewnienie zgodnego z prawem, rzetelnego, przejrzystego i bezpiecznego przetwarzania danych osobowych oraz ograniczenie ryzyka ich utraty, uszkodzenia, zmiany, nieuprawnionego ujawnienia lub dostępu.
3. Polityka obowiązuje:

- członków Zarządu Fundacji;
- pracowników;
- współpracowników;
- osoby zatrudnione na podstawie umów cywilnoprawnych;
- wolontariuszy;
- praktykantów;
- stażystów;
- osoby prowadzące warsztaty, szkolenia i projekty;
- osoby posiadające dostęp do systemów informatycznych, dokumentacji papierowej lub danych osobowych przetwarzanych przez Fundację.

4. Każda osoba dopuszczona do przetwarzania danych osobowych zobowiązana jest do przestrzegania niniejszej Polityki.

---

§ 2. Podstawy prawne

Polityka została opracowana na podstawie:

1. rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, zwanego dalej „RODO";
2. ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;

3. Kodeksu pracy;
4. ustawy o rachunkowości;
5. przepisów podatkowych i ubezpieczeniowych;
6. ustawy o działalności pożytku publicznego i o wolontariacie;
7. przepisów dotyczących realizowanych przez Fundację projektów, dotacji i zadań publicznych;
8. innych przepisów mających zastosowanie do działalności Fundacji.

Rozdział II

Definicje

§ 3

Ilekroć w Polityce jest mowa o:

Administratorze – należy przez to rozumieć Fundację Bez Lukru i Cukru, która ustala cele i sposoby przetwarzania danych osobowych;

Fundacji – należy przez to rozumieć Fundację Bez Lukru i Cukru;

Zarządzie – należy przez to rozumieć Zarząd Fundacji Bez Lukru i Cukru;

danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

danych szczególnych kategorii – należy przez to rozumieć w szczególności dane dotyczące zdrowia, niepełnosprawności, pochodzenia rasowego lub etnicznego, przekonań religijnych, poglądów politycznych, danych genetycznych, biometrycznych oraz życia seksualnego;

przetwarzaniu – należy przez to rozumieć każdą operację wykonywaną na danych osobowych, w szczególności zbieranie, utrwalanie, porządkowanie, przechowywanie, modyfikowanie, przeglądanie, wykorzystywanie, przesyłanie, udostępnianie, ograniczanie, usuwanie lub niszczenie;

systemie informatycznym – należy przez to rozumieć urządzenia, programy, aplikacje, konta internetowe i usługi wykorzystywane do przetwarzania danych;

osobie upoważnionej – należy przez to rozumieć osobę, której Administrator udzielił upoważnienia do przetwarzania danych osobowych;

podmiocie przetwarzającym – należy przez to rozumieć podmiot przetwarzający dane osobowe w imieniu Fundacji, np. biuro rachunkowe, firma informatyczna, dostawca hostingu lub systemu informatycznego;

naruszeniu ochrony danych osobowych – należy przez to rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, ujawnienia lub uzyskania dostępu do danych osobowych;

nośniku danych – należy przez to rozumieć dokument papierowy, komputer, telefon, dysk, pendrive, kartę pamięci, płytę, chmurę lub inne miejsce przechowywania danych.

Rozdział III

Administrator danych osobowych

§ 4

1. Administratorem danych osobowych jest:

Fundacja Bez Lukru i Cukru

adres siedziby:
ul. Piaskowa 1M, 26-660 Wielogóra

KRS:
0001154192

NIP:
9482651136

REGON:
540850000

adres e-mail:
fundacjabezlukruicukru@gmail.com

numer telefonu:
883971991

2. Administrator odpowiada za:

- zgodność przetwarzania danych z przepisami prawa;
- wdrożenie odpowiednich środków organizacyjnych i technicznych;
- zapewnienie rozliczalności przetwarzania;
- prowadzenie wymaganej dokumentacji;
- nadawanie i odbieranie upoważnień;
- prowadzenie rejestru czynności przetwarzania;
- zawieranie umów powierzenia przetwarzania;
- realizację praw osób, których dane dotyczą;
- analizę ryzyka;

- reagowanie na naruszenia;
- przeprowadzanie szkoleń personelu.

3. Zadania Administratora wykonuje Zarząd Fundacji lub osoba pisemnie wyznaczona przez Zarząd.

---

§ 5. Inspektor ochrony danych

1. Fundacja dokonuje oceny, czy zachodzi obowiązek wyznaczenia Inspektora Ochrony Danych.
2. Jeżeli obowiązek taki nie zachodzi, Fundacja może dobrowolnie wyznaczyć Inspektora Ochrony Danych lub osobę koordynującą ochronę danych.
3. Jeżeli Inspektor Ochrony Danych zostanie wyznaczony, jego dane kontaktowe są publikowane zgodnie z przepisami i przekazywane Prezesowi Urzędu Ochrony Danych Osobowych.
4. W przypadku niewyznaczenia Inspektora sprawami ochrony danych zajmuje się Zarząd albo osoba przez niego upoważniona.

Rozdział IV

Zasady przetwarzania danych

§ 6

Fundacja przetwarza dane osobowe zgodnie z następującymi zasadami:

1. **zgodności z prawem, rzetelności i przejrzystości** – dane przetwarzane są na właściwej podstawie prawnej i w sposób zrozumiały dla osoby, której dotyczą;
2. **ograniczenia celu** – dane zbierane są wyłącznie w konkretnych i zgodnych z prawem celach;
3. **minimalizacji danych** – zbierane są tylko dane niezbędne;
4. **prawidłowości** – dane powinny być aktualne i poprawne;
5. **ograniczenia przechowywania** – dane przechowywane są nie dłużej, niż jest to niezbędne;
6. **integralności i poufności** – dane zabezpiecza się przed nieuprawnionym dostępem, utratą i zniszczeniem;
7. **rozliczalności** – Fundacja jest w stanie wykazać przestrzeganie przepisów.

Rozdział V

Kategorie osób i zakres przetwarzanych danych

§ 7

Fundacja może przetwarzać dane dotyczące następujących kategorii osób:

1. członków organów Fundacji;
2. pracowników;
3. kandydatów do pracy;
4. współpracowników i zleceniobiorców;
5. wolontariuszy, stażystów i praktykantów;
6. beneficjentów projektów;
7. dzieci i młodzieży uczestniczących w zajęciach;
8. rodziców i opiekunów prawnych;
9. uczestników wydarzeń, warsztatów i szkoleń;
10. klientów kawiarni, cukierni, cateringu oraz innych usług Fundacji;
11. kontrahentów i dostawców;
12. darczyńców;
13. osób przekazujących darowizny;
14. osób kontaktujących się z Fundacją;
15. odbiorców newslettera;
16. obserwujących profile Fundacji w mediach społecznościowych;
17. osób utrwalonych na zdjęciach i nagraniach;
18. osób zgłaszających skargi, wnioski lub naruszenia;
19. osób objętych dokumentacją projektową, księgową, kadrową lub reintegracyjną.

---

§ 8

Fundacja może przetwarzać w szczególności:

- imię i nazwisko;
- datę urodzenia;
- PESEL;
- adres zamieszkania;
- adres korespondencyjny;
- adres e-mail;
- numer telefonu;
- dane dotyczące wykształcenia i kwalifikacji;
- dane o zatrudnieniu;
- dane rachunku bankowego;
- dane podatkowe i ubezpieczeniowe;
- dane zawarte w umowach;

- dane dotyczące udziału w projektach;
- dane o niepełnosprawności lub stanie zdrowia, jeśli są niezbędne i istnieje właściwa podstawa prawna;
- dane rodziców i opiekunów;
- wizerunek;
- głos;
- informacje dotyczące szczególnych potrzeb uczestnika;
- dane dotyczące bezrobotności, zatrudnienia, sytuacji społecznej lub ekonomicznej wymagane w projektach;
- dane dotyczące zamówień, płatności, reklamacji i kontaktu z Fundacją.

Rozdział VI

Podstawy przetwarzania danych

§ 9

Fundacja przetwarza dane osobowe, gdy:

1. jest to niezbędne do wykonania umowy lub podjęcia działań przed zawarciem umowy;
2. jest to niezbędne do wypełnienia obowiązku prawnego;
3. osoba wyraziła zgodę;
4. przetwarzanie jest konieczne do ochrony żywotnych interesów osoby;
5. jest to niezbędne do wykonania zadania realizowanego w interesie publicznym;
6. jest to niezbędne do celów wynikających z prawnie uzasadnionych interesów Fundacji, z wyjątkiem sytuacji, w których nadrzędny charakter mają prawa i wolności osoby.

---

§ 10

Dane szczególnych kategorii przetwarzane są wyłącznie wtedy, gdy istnieje właściwa podstawa prawna, w szczególności:

- wyraźna zgoda osoby;
- obowiązek wynikający z prawa pracy lub zabezpieczenia społecznego;
- konieczność ochrony żywotnych interesów;
- realizacja szczególnych zadań statutowych przez Fundację;
- ustalenie, dochodzenie lub obrona roszczeń;
- ważny interes publiczny;
- obowiązki wynikające z realizacji projektu lub zadania publicznego.

Rozdział VII

Obowiązek informacyjny

§ 11

1. Fundacja przekazuje osobom, których dane zbiera, odpowiednią klauzulę informacyjną.
2. Klauzula powinna zawierać w szczególności:

- dane Administratora;
- dane kontaktowe osoby odpowiedzialnej za ochronę danych lub IOD, jeżeli został wyznaczony;
- cele przetwarzania;
- podstawy prawne;
- informacje o odbiorcach danych;
- okres przechowywania;
- prawa osoby;
- informację o prawie wniesienia skargi do Prezesa UODO;
- informację, czy podanie danych jest obowiązkowe;
- informację o zautomatyzowanym podejmowaniu decyzji;
- informację o przekazywaniu danych poza Europejski Obszar Gospodarczy.

3. Jeżeli dane nie są pozyskiwane bezpośrednio od osoby, obowiązek informacyjny realizowany jest zgodnie z art. 14 RODO.
4. Fundacja opracowuje odrębne klauzule informacyjne m.in. dla:

- pracowników;
- kandydatów do pracy;
- wolontariuszy;
- uczestników projektów;
- dzieci i rodziców;
- klientów;
- kontrahentów;
- darczyńców;
- osób korzystających ze strony internetowej;
- odbiorców newslettera;
- osób utrwalanych na zdjęciach i nagraniach.

Rozdział VIII

Prawa osób, których dane dotyczą

§ 12

Osobie, której dane dotyczą, może przysługiwać prawo do:

- dostępu do danych;
- otrzymania kopii danych;
- sprostowania danych;
- usunięcia danych;
- ograniczenia przetwarzania;
- przenoszenia danych;
- wniesienia sprzeciwu;
- wycofania zgody;
- niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu;
- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

---

§ 13

1. Wnioski dotyczące realizacji praw mogą być składane pisemnie lub elektronicznie.
2. Przed realizacją wniosku Fundacja może zweryfikować tożsamość osoby.
3. Fundacja odpowiada na wniosek bez zbędnej zwłoki, zasadniczo w terminie jednego miesiąca.
4. Każdy wniosek jest rejestrowany.
5. Fundacja prowadzi rejestr realizacji praw osób.

Rozdział IX

Upoważnienia do przetwarzania danych

§ 14

1. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie Administratora.
2. Upoważnienie określa:

- imię i nazwisko osoby;
- zakres danych;
- zakres czynności;
- systemy i dokumentację, do których osoba ma dostęp;
- datę nadania;

- okres obowiązywania.

3. Upoważnienie może mieć formę papierową lub elektroniczną.
4. Fundacja prowadzi ewidencję osób upoważnionych.
5. Upoważnienie wygasa w szczególności:

- z chwilą zakończenia zatrudnienia lub współpracy;
- po zmianie stanowiska;
- po utracie potrzeby dostępu;
- po cofnięciu upoważnienia.

6. Po wygaśnięciu upoważnienia dostęp do systemów i dokumentacji jest niezwłocznie odbierany.

---

§ 15

Osoba upoważniona zobowiązana jest:

- przetwarzać dane wyłącznie na polecenie Administratora;
- zachować poufność;
- nie udostępniać danych osobom nieuprawnionym;
- stosować zabezpieczenia;
- chronić hasła;
- zgłaszać naruszenia;
- nie wynosić dokumentacji bez zgody;
- nie wykorzystywać danych do celów prywatnych;
- przestrzegać zasad korzystania ze sprzętu służbowego.

Obowiązek zachowania poufności trwa także po zakończeniu zatrudnienia lub współpracy.

Rozdział X

Rejestr czynności przetwarzania

§ 16

1. Fundacja prowadzi rejestr czynności przetwarzania.
2. Rejestr obejmuje w szczególności:

- nazwę czynności;
- cel przetwarzania;
- kategorię osób;
- kategorię danych;
- podstawę prawną;

- odbiorców danych;
- informacje o przekazywaniu danych poza Europejski Obszar Gospodarczy;
- okres przechowywania;
- opis zabezpieczeń.

3. Rejestr podlega aktualizacji w razie zmiany działalności Fundacji.
4. Przykładowe czynności przetwarzania:

- obsługa zatrudnienia;
- prowadzenie rekrutacji;
- obsługa wolontariatu;
- realizacja projektów;
- prowadzenie zajęć dla dzieci;
- realizacja warsztatów;
- obsługa klientów;
- prowadzenie rachunkowości;
- obsługa darowizn;
- prowadzenie strony internetowej;
- publikacja wizerunku;
- prowadzenie mediów społecznościowych;
- obsługa korespondencji;
- rozpatrywanie skarg i reklamacji.

Rozdział XI

Powierzenie przetwarzania danych

§ 17

1. Jeżeli inny podmiot przetwarza dane w imieniu Fundacji, zawierana jest umowa powierzenia przetwarzania danych.
2. Umowę zawiera się w szczególności z:

- biurem rachunkowym;
- dostawcą systemu kadrowego;
- dostawcą hostingu;
- dostawcą poczty elektronicznej;
- firmą informatyczną;
- dostawcą systemu rejestracji uczestników;
- podmiotem prowadzącym archiwizację lub niszczenie dokumentacji;
- podmiotem realizującym wysyłkę newslettera;
- podwykonawcą mającym dostęp do danych.

3. Przed powierzeniem danych Fundacja ocenia, czy podmiot zapewnia odpowiednie zabezpieczenia.
4. Fundacja prowadzi wykaz podmiotów przetwarzających.

Rozdział XII

Udostępnianie danych

§ 18

1. Dane mogą być udostępniane wyłącznie:

- osobie, której dane dotyczą;
- osobie posiadającej upoważnienie;
- podmiotowi przetwarzającemu;
- instytucji uprawnionej na podstawie prawa;
- grantodawcy lub instytucji kontrolującej, jeżeli wynika to z dokumentacji projektu;
- sądom, Policji, prokuraturze, urzędom skarbowym, ZUS, PFRON, urzędom pracy i innym właściwym instytucjom;
- innym odbiorcom, jeżeli istnieje odpowiednia podstawa prawna.

2. Przed udostępnieniem danych weryfikuje się tożsamość i uprawnienie odbiorcy.
3. Dane przekazuje się w zakresie niezbędnym.
4. W przypadku wątpliwości pracownik wstrzymuje udostępnienie i konsultuje sprawę z Zarządem.

Rozdział XIII

Okresy przechowywania danych

§ 19

1. Dane przechowywane są przez okres niezbędny do realizacji celu oraz zgodnie z przepisami prawa.
2. Okresy przechowywania ustala się osobno dla poszczególnych procesów.
3. Dokumentacja pracownicza przechowywana jest przez okres wynikający z przepisów prawa pracy.
4. Dokumentacja księgowa i podatkowa przechowywana jest przez okres wymagany przepisami.
5. Dokumentacja projektowa przechowywana jest przez okres wskazany w umowie, regulaminie projektu lub przepisach dotyczących finansowania.
6. Dane przetwarzane na podstawie zgody przechowywane są do czasu:

- wycofania zgody;
- realizacji celu;
- upływu ustalonego okresu;
- skutecznego zgłoszenia sprzeciwu, gdy ma zastosowanie.

7. Dane mogą być przechowywane dłużej, jeżeli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń.
8. Fundacja prowadzi harmonogram retencji danych.
9. Po upływie okresu przechowywania dane są usuwane, anonimizowane albo dokumentacja jest niszczona.

Rozdział XIV

Zabezpieczenie dokumentacji papierowej

§ 20

Dokumentacja papierowa zawierająca dane osobowe:

- przechowywana jest w zamykanych szafach lub pomieszczeniach;
- nie jest pozostawiana bez nadzoru w miejscach ogólnodostępnych;
- nie jest udostępniana osobom nieuprawnionym;
- transportowana jest w sposób zabezpieczony;
- po wykorzystaniu odkładana jest do właściwego miejsca;
- niszczona jest za pomocą niszczarki lub przez wyspecjalizowany podmiot;
- nie może być wyrzucana do zwykłego kosza.

---

§ 21. Zasada czystego biurka

1. Po zakończeniu pracy dokumenty zawierające dane osobowe należy zabezpieczyć.
2. Dokumentów nie pozostawia się:

- na biurku;
- przy drukarce;
- w sali warsztatowej;
- na ladzie;
- w samochodzie;
- w ogólnodostępnym pomieszczeniu.

3. Wydruki należy odbierać z drukarki bez zbędnej zwłoki.

Rozdział XV

Zabezpieczenie systemów informatycznych

§ 22

Fundacja stosuje odpowiednie środki zabezpieczające, w szczególności:

- indywidualne konta użytkowników;
- silne hasła;
- uwierzytelnianie wieloskładnikowe, gdy jest dostępne;
- programy antywirusowe;
- zapory sieciowe;
- aktualizację oprogramowania;
- szyfrowanie urządzeń lub nośników, gdy jest to uzasadnione;
- automatyczne blokowanie ekranów;
- tworzenie kopii zapasowych;
- ograniczenie uprawnień;
- zabezpieczenie sieci Wi-Fi;
- kontrolę dostępu do chmury i poczty elektronicznej.

---

§ 23. Hasła

1. Hasła powinny być trudne do odgadnięcia.
2. Zabronione jest:

- udostępnianie hasła innej osobie;
- zapisywanie hasła w widocznym miejscu;
- przesyłanie hasła niezabezpieczonym kanałem;
- używanie jednego hasła do wielu ważnych usług;
- używanie prostych haseł zawierających imię, nazwę Fundacji lub datę urodzenia.

3. Hasło należy zmienić niezwłocznie w przypadku podejrzenia jego ujawnienia.

---

§ 24. Poczta elektroniczna

1. Przed wysłaniem wiadomości należy sprawdzić:

- adresata;
- załączniki;
- zakres przekazywanych danych;
- czy wiadomość nie zawiera danych innej osoby.

2. Przy wysyłce do wielu niezależnych odbiorców należy stosować pole „UDW”, chyba że odbiorcy mogą znać swoje adresy.
3. Dokumenty zawierające dane szczególnie chronione powinny być zabezpieczone hasłem, jeżeli wymaga tego ocena ryzyka.
4. Hasło powinno zostać przekazane innym kanałem.
5. Zabrania się automatycznego przekazywania poczty służbowej na prywatne skrzynki.

---

§ 25. Urządzenia mobilne

1. Telefony, laptopy i tablety wykorzystywane do przetwarzania danych powinny być zabezpieczone hasłem, kodem lub inną metodą uwierzytelniania.
2. Urządzeń nie pozostawia się bez nadzoru.
3. W przypadku utraty urządzenia osoba zobowiązana jest niezwłocznie poinformować Zarząd.
4. Na urządzeniach prywatnych dane mogą być przetwarzane wyłącznie po uzyskaniu zgody i zastosowaniu wymaganych zabezpieczeń.

Rozdział XVI

Praca poza siedzibą Fundacji

§ 26

1. Podczas pracy zdalnej lub wyjazdowej należy zapewnić, aby osoby postronne nie miały dostępu do danych.
2. Zabronione jest prowadzenie rozmów o danych osobowych w miejscach publicznych w sposób umożliwiający ich usłyszenie.
3. Dokumentów zawierających dane nie pozostawia się w samochodzie.
4. Podczas warsztatów i projektów listy uczestników, zgody, formularze i dzienniki należy przechowywać pod nadzorem prowadzącego.
5. Po zakończeniu wydarzenia dokumentacja powinna zostać przekazana osobie odpowiedzialnej lub zabezpieczona w siedzibie Fundacji.

Rozdział XVII

Kopie zapasowe i ciągłość działania

§ 27

1. Dla danych niezbędnych do działalności Fundacji wykonuje się kopie zapasowe.
2. Kopie tworzone są z częstotliwością dostosowaną do znaczenia danych.
3. Kopie zapasowe przechowywane są w sposób zabezpieczony i – jeśli jest to możliwe – w lokalizacji innej niż dane podstawowe.
4. Dostęp do kopii mają wyłącznie osoby upoważnione.
5. Okresowo sprawdza się możliwość odtworzenia danych.

Rozdział XVIII

Naruszenia ochrony danych osobowych

§ 28

Naruszeniem może być w szczególności:

- wysłanie wiadomości do niewłaściwego adresata;
- utrata dokumentów;
- kradzież komputera lub telefonu;
- zgubienie pendrive’a;
- ujawnienie danych osobie nieuprawnionej;
- włamanie do systemu;
- zainfekowanie urządzenia;
- utrata dostępu do danych;
- przypadkowe usunięcie danych;
- opublikowanie danych lub wizerunku bez podstawy;
- pozostawienie dokumentów w miejscu publicznym;
- użycie funkcji „DW” zamiast „UDW”;
- nieuprawniony dostęp pracownika.

---

§ 29

1. Każda osoba, która zauważyła lub podejrzewa naruszenie, ma obowiązek natychmiast zgłosić je Zarządowi.
2. Zgłoszenie powinno zawierać, o ile jest to możliwe:

- datę i godzinę zdarzenia;
- opis zdarzenia;

- rodzaj danych;
- liczbę osób;
- możliwe skutki;
- podjęte działania;
- informację, komu dane mogły zostać ujawnione.

3. Nie należy samodzielnie ukrywać ani usuwać skutków naruszenia bez uzgodnienia.
4. Zarząd zabezpiecza dowody i podejmuje działania ograniczające skutki.

---

§ 30

1. Fundacja prowadzi rejestr naruszeń.
2. Każde naruszenie podlega ocenie pod względem ryzyka dla praw i wolności osób.
3. Jeżeli naruszenie może powodować ryzyko naruszenia praw lub wolności osób, Administrator zgłasza je Prezesowi UODO bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 72 godzin od stwierdzenia.
4. Jeżeli naruszenie może powodować wysokie ryzyko dla osoby, Fundacja zawiadamia również tę osobę, chyba że zachodzi ustawowy wyjątek.
5. Jeżeli naruszenie nie podlega zgłoszeniu, przyczyny tej decyzji są dokumentowane.

Rozdział XIX

Analiza ryzyka

§ 31

1. Fundacja okresowo przeprowadza analizę ryzyka związanego z przetwarzaniem danych osobowych.
2. Przy ocenie ryzyka uwzględnia się:

- rodzaj danych;
- liczbę osób;
- zakres danych;
- sposób przetwarzania;
- miejsce przechowywania;
- możliwość utraty;
- skutki dla osoby;
- dostęp osób trzecich;
- korzystanie z usług zewnętrznych;
- przetwarzanie danych dzieci;
- przetwarzanie danych o zdrowiu lub niepełnosprawności.

3. Na podstawie analizy Fundacja wdraża odpowiednie zabezpieczenia.
4. Analizę aktualizuje się:

- po zmianie systemu;
- po rozpoczęciu nowego projektu;
- po wystąpieniu naruszenia;
- po zmianie sposobu przetwarzania;
- okresowo, nie rzadziej niż raz na dwa lata.

Rozdział XX

Ocena skutków dla ochrony danych

§ 32

1. Jeżeli planowany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób, Fundacja przeprowadza ocenę skutków dla ochrony danych.
2. Ocena może być wymagana w szczególności przy:

- przetwarzaniu na dużą skalę danych o zdrowiu;
- systematycznym monitorowaniu osób;
- wdrażaniu nowych technologii;
- profilowaniu;
- przetwarzaniu dużej liczby danych dzieci;
- łączeniu wielu baz danych.

Rozdział XXI

Dane dzieci i młodzieży

§ 33

1. Dane dzieci objęte są szczególną ochroną.
2. Fundacja zbiera wyłącznie dane niezbędne do:

- organizacji zajęć;
- kontaktu z opiekunem;
- zapewnienia bezpieczeństwa;
- realizacji projektu;
- rozliczenia dotacji;
- udokumentowania udziału;
- zapewnienia dostępności i szczególnego wsparcia.

3. Dostęp do danych dzieci mają wyłącznie osoby, które potrzebują ich do wykonywania obowiązków.

4. Dane dotyczące zdrowia, niepełnosprawności, alergii lub szczególnych potrzeb przetwarzane są tylko w zakresie niezbędnym.
5. List uczestników nie publikuje się publicznie bez podstawy prawnej.
6. Dokumentacja dzieci nie może być przechowywana w ogólnodostępnym miejscu.

Rozdział XXII

Wizerunek

§ 34

1. Utrwalanie i rozpowszechnianie wizerunku odbywa się zgodnie z przepisami prawa.
2. Jeżeli wymagana jest zgoda, musi ona być:

- dobrowolna;
- konkretna;
- świadoma;
- jednoznaczna;
- możliwa do wycofania.

3. Zgoda na udział w projekcie nie oznacza automatycznie zgody na publikację wizerunku.
4. W przypadku dzieci zgody udziela rodzic lub opiekun prawny, a w miarę możliwości uwzględnia się również zdanie dziecka.
5. Fundacja unika publikowania:

- pełnego imienia i nazwiska dziecka wraz ze zdjęciem;
- informacji o stanie zdrowia;
- danych szkoły, adresu i szczegółów pozwalających ustalić miejsce pobytu;
- materiałów naruszających godność dziecka.

6. Zgody na wykorzystanie wizerunku są ewidencjonowane.

Rozdział XXIII

Media społecznościowe i strona internetowa

§ 35

1. Osoby prowadzące profile Fundacji publikują treści zgodnie z udzielonym zakresem uprawnień.
2. Dostęp administracyjny do profili powinien być ograniczony.
3. Stosuje się uwierzytelnianie wieloskładnikowe, gdy jest dostępne.
4. Po zakończeniu współpracy dostęp do profili jest odbierany.
5. Nie publikuje się danych osobowych w komentarzach ani wiadomościach publicznych.
6. Wiadomości prywatne zawierające dane osobowe należy obsługiwać zgodnie z zasadami poufności.
7. Formularze na stronie internetowej powinny zawierać odpowiednią klauzulę informacyjną.

Rozdział XXIV

Monitoring przestrzegania Polityki

§ 36

1. Zarząd monitoruje przestrzeganie niniejszej Polityki.
2. Kontrola może obejmować:

- dokumentację;
- upoważnienia;
- systemy informatyczne;
- konta użytkowników;
- zabezpieczenia pomieszczeń;
- umowy powierzenia;
- retencję danych;
- realizację praw osób;
- rejestr naruszeń.

3. Naruszenie Polityki może skutkować:

- upomnieniem;
- odebraniem uprawnień;
- odpowiedzialnością pracowniczą lub cywilną;
- zakończeniem współpracy;
- zawiadomieniem właściwych organów.

Rozdział XXV

Szkolenia

§ 37

1. Osoby przetwarzające dane są szkolone przed uzyskaniem dostępu do danych.
2. Szkolenie obejmuje w szczególności:

- podstawowe zasady RODO;
- obowiązek poufności;
- zasady korzystania z poczty;
- zasady ochrony dokumentacji;
- reagowanie na naruszenia;
- zasady ochrony danych dzieci;
- ochronę haseł;
- zasady pracy zdalnej.

3. Przeprowadzenie szkolenia jest dokumentowane.
4. Szkolenia są powtarzane okresowo oraz po istotnej zmianie zasad.

Rozdział XXVI

Przegląd dokumentacji

§ 38

1. Polityka podlega przeglądowi nie rzadziej niż raz na dwa lata.
2. Politykę aktualizuje się również:

- po zmianie przepisów;
- po zmianie struktury Fundacji;
- po wdrożeniu nowego systemu;
- po rozpoczęciu nowego rodzaju działalności;
- po poważnym naruszeniu;
- po zmianie zakresu przetwarzanych danych.

3. Za aktualizację odpowiada Zarząd.

Rozdział XXVII

Postanowienia końcowe

§ 39

1. Polityka wchodzi w życie z dniem przyjęcia jej uchwałą lub zarządzeniem Zarządu Fundacji Bez Lukru i Cukru.
2. Każda osoba dopuszczona do przetwarzania danych potwierdza zapoznanie się z Polityką.
3. Integralną częścią dokumentacji ochrony danych powinny być:

1. rejestr czynności przetwarzania;
2. ewidencja osób upoważnionych;
3. wzór upoważnienia do przetwarzania danych;
4. oświadczenie o zachowaniu poufności;
5. wykaz podmiotów przetwarzających;
6. wzór umowy powierzenia;
7. rejestr naruszeń;
8. formularz zgłoszenia naruszenia;
9. rejestr realizacji praw osób;
10. procedura realizacji praw osób;
11. harmonogram retencji danych;
12. analiza ryzyka;
13. wykaz systemów informatycznych;
14. wykaz miejsc przetwarzania danych;
15. procedura tworzenia kopii zapasowych;
16. klauzule informacyjne;
17. wzory zgód na wykorzystanie wizerunku;
18. procedura nadawania i odbierania dostępów;
19. protokół usunięcia lub zniszczenia danych;
20. rejestr szkoleń.

ZATWIERDZENIE POLITYKI

Polityka bezpieczeństwa danych osobowych została przyjęta przez Zarząd Fundacji Bez Lukru i Cukru w dniu:

.....

Numer uchwały/zarządzenia:

.....

Podpisy członków Zarządu:

.....

.....

ZAŁĄCZNIK NR 1

Upoważnienie do przetwarzania danych osobowych

Fundacja Bez Lukru i Cukru upoważnia:

Imię i nazwisko:
.....

Stanowisko/funkcja:
.....

do przetwarzania danych osobowych w zakresie:

.....

.....

Upoważnienie obejmuje następujące systemy, dokumenty lub zbiory:

.....

Upoważnienie obowiązuje od:

.....

do dnia odwołania / do dnia:

.....

Osoba upoważniona zobowiązana jest do zachowania danych osobowych w poufności oraz przestrzegania Polityki bezpieczeństwa danych osobowych.

Data i podpis Administratora:

.....

Podpis osoby upoważnionej:

.....

ZAŁĄCZNIK NR 2

Oświadczenie o zachowaniu poufności

Ja,

.....

oświadczam, że:

1. zapoznałem/am się z Polityką bezpieczeństwa danych osobowych Fundacji Bez Lukru i Cukru;
2. zobowiązuję się do przetwarzania danych wyłącznie w zakresie udzielonego upoważnienia;
3. zobowiązuję się do zachowania danych osobowych oraz sposobów ich zabezpieczenia w poufności;
4. nie będę udostępniać danych osobom nieuprawnionym;
5. będę niezwłocznie zgłaszać każde podejrzenie naruszenia ochrony danych;
6. obowiązek poufności zachowuję również po zakończeniu zatrudnienia lub współpracy.

Data:

.....

Podpis:

.....

ZAŁĄCZNIK NR 3

Formularz zgłoszenia naruszenia

Data i godzina stwierdzenia zdarzenia:
.....

Osoba zgłaszająca:
.....

Opis zdarzenia:

.....

.....

Rodzaj danych objętych zdarzeniem:

.....

Liczba osób, których dane mogą dotyczyć:

.....

Osoby lub podmioty, którym dane mogły zostać ujawnione:

.....

Możliwe skutki:

.....

Podjęte działania zabezpieczające:

.....

Data i podpis osoby zgłaszającej:

.....

ZAŁĄCZNIK NR 4

Rejestr naruszeń

1. Numer naruszenia:
   .....
2. Data zdarzenia:
   .....
3. Data stwierdzenia:
   .....
4. Opis naruszenia:
   .....
5. Kategorie danych:
   .....
6. Liczba osób:
   .....
7. Ocena ryzyka:
   .....
8. Zastosowane środki:
   .....
9. Czy zgłoszono do Prezesa UODO:
   TAK / NIE

10. Data zgłoszenia:
    .....
11. Czy zawiadomiono osoby:
    TAK / NIE
12. Uzasadnienie decyzji:
    .....

ZAŁĄCZNIK NR 5

Ewidencja osób upoważnionych

Lp.: .....

Imię i nazwisko:
.....

Stanowisko/funkcja:
.....

Zakres upoważnienia:
.....

Data nadania:
.....

Data cofnięcia:
.....

Podpis osoby upoważnionej:
.....

ZAŁĄCZNIK NR 6

Protokół odebrania dostępu

Imię i nazwisko osoby:

.....

Data zakończenia współpracy lub zmiany zakresu obowiązków:

.....

Odebrano:

- dostęp do poczty: TAK / NIE / NIE DOTYCZY;
- dostęp do dysku lub chmury: TAK / NIE / NIE DOTYCZY;
- dostęp do mediów społecznościowych: TAK / NIE / NIE DOTYCZY;
- dostęp do systemów projektowych: TAK / NIE / NIE DOTYCZY;
- klucze: TAK / NIE / NIE DOTYCZY;
- sprzęt: TAK / NIE / NIE DOTYCZY;
- dokumentację: TAK / NIE / NIE DOTYCZY;
- inne dostępy:

.....

Data i podpis osoby odbierającej:

.....